

FIPS 140-2, IEEE 802.11i and WPA2  
In 3eTI Wireless Products

R. K. Coleman

**3e Technologies International, Inc.**  
9715 Key West Avenue, Fifth Floor  
Rockville, MD 20850

## **Abstract**

IEEE 802.11i goes beyond the simple, flawed encryption mechanism of 1999 IEEE 802.11 WEP to include specifications on encryption, authentication and key management in a multi-layered approach to security. Both WPA and WPA2 protect the wireless network from a variety of threats, including lost or stolen devices and hacker attacks such as ‘man-in-the-middle’, authentication forging, replay, key collision, weak keys, packet forging, and ‘brute-force/dictionary’ attacks. While WPA relies on the older RC4 stream cipher for encryption, WPA2 is the second generation of WPA security; providing enterprise and consumer Wi-Fi® users with a high level of assurance that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard, employs AES for data encryption, and is eligible for FIPS 140-2 compliance. FIPS 140-2 is the Federal Information Processing Standard for cryptography. It defines a set of cryptographic functions approved for protection of sensitive but unclassified data in the U.S. Government, and provides guidelines governing the correct implementation and deployment of these functions. On January 21, 2005, NIST issued an updated implementation guidance document for FIPS 140-2. Section 7.2 of this update addresses IEEE Std 802.11i. It indicates that an IEEE Std. 802.11i deployment can be certified and deployed for sensitive but unclassified use. This paper discusses these points, and highlights the fact that 3eTI wireless access points (3e-525A2.3), client devices, and the security server have been designed to be FIPS 140-2 certified, 802.11i compliant, and also WPA2 certified; thereby providing extremely high levels of security to the enterprise customer, while ensuring interoperability with the spectrum of cost-competitive, COTS, WPA2 certified wireless equipment available in the marketplace.

## **Overview of IEEE 802.11i and 3eTI Product Implementations**

IEEE 802.11i goes beyond the simple, flawed encryption mechanism of 1999 802.11 WEP to include specifications on encryption, authentication and key management in a multi-layered approach to security. IEEE 802.1X-based authentication mechanisms are used, with AES in CCMP mode, to establish an 802.11 Robust Security Network (RSN). IEEE 802.1X defines a framework based on the Extensible Authentication Protocol (EAP) over LANs, also known as EAPoL. EAPoL is used to exchange EAP messages. These EAP messages execute an authentication sequence and are used for key derivation between a Station (STA) and an EAP entity known as the Authentication Server (AS). IEEE 802.11i defines a four-way handshake using EAPoL for key management and pairwise and group key derivation. 3eTI has been instrumental in developing an IETF RFC to further standardize the portion of key exchange that must take place between the Authentication Server and the Wireless Access Point (WAP). 3eTI, along with Cisco and Intel, recognizes the merits of standardizing this technique, so that interoperability among multiple 802.11i-compliant vendors can be achieved.

Four major categories or primary functions of 802.11i are invoked within 3eTI products, including the wireless client devices, wireless access points (3e-525A2.3), and the security server. These primary functions of 802.11i include:

1. EAP-TLS: Extensible Authentication Protocol Transport Layer Security, EAP-TLS was compulsory for WPA2 Enterprise products certified prior to April 15, 2005; for products certified after this date, EAP-TLS testing is compulsory if the product can support EAP-TLS. The only products that might not support EAP-TLS are tightly integrated systems that do not support software upgrades by a third party, such as some cell phones intended for, e.g., the 3G market. Non-tightly integrated products like most laptop and PDU adapters still must support EAP-TLS to receive WPA2 certification. 3eTI wireless client and wireless access point devices use standards-based EAP-TLS with no modifications, for complete interoperability with 802.11i and WPA2 certified equipment.
2. IEEE 802.1X: also known as port based network access control, 802.1X provides and authentication framework within 802.11i. 802.11i depends upon 802.1X to control the flow of MSDUs between the DS and STAs by use of the IEEE 802.1X Controlled/Uncontrolled Port model. IEEE 802.1X authentication frames are transmitted in 802.11 Data frames and passed via the IEEE 802.1X Uncontrolled Port. The 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an 802.1X authentication procedure completes successfully over the 802.1X Uncontrolled Port. It is the responsibility of both the Supplicant (3eTI wireless client device) and the Authenticator (3eTI security server) to implement port blocking. 802.11 depends upon IEEE 802.1X and the EAPOL-Key 4-Way and Group Key Handshakes, to establish and change cryptographic keys. Keys are established after authentication has completed. Keys may change for a variety of reasons, including expiration of an IEEE 802.1X authentication timer, key compromise, danger of compromise, or policy. 3eTI products implement standards-based 802.1X with absolutely no custom modifications, again ensuring interoperability with 802.11i and WPA2 certified equipment.
3. 4-way handshake: The 4-way handshake defined in 802.11i achieves the following important goals within the security protocol:
  - a. it confirms the PMK between the supplicant (3e client) and authenticator (3e security server)
  - b. it establishes the temporal keys to be used by the data-confidentiality protocol
  - c. it authenticates the security parameters that were negotiated
  - d. it performs the first group key handshake within 802.11i
  - e. it provides keying material to implement the group key handshake within 802.11i

3eTI implements the 4-way handshake within its wireless product line per the 802.11i specification, again with absolutely no custom modifications, in order to maximize interoperability with 3<sup>rd</sup> party 802.11i and WPA2 compliant equipment.

4. AES CCMP: 802.11i and WPA2 employ AES CCM, which is a combination of AES Counter (CTR) mode per packet data encryption, combined with AES Cipher Block Chaining – Message Authentication Code (CBC-MAC) per packet data integrity / authentication of the entire packet including the MAC header. AES CCMP has been deemed to surpass the RC4 stream cipher, upon which the older WEP and WPA security protocols are based. 3eTI was the first company to take it's AES algorithm through the NIST CCM algorithm certification process, thereby ensuring that 3eTI's AES CCMP is standards-based, non-proprietary, and ready for wide WPA2 interoperability usage.

Refer to: <http://csrc.nist.gov/cryptval/mac/ccmval.html> for details on the certificate.

## Highlights of FIPS 140-2

FIPS 140-2 is the Federal Information Processing Standard for cryptography. It defines a set of cryptographic functions approved for protecting of sensitive but unclassified data in the U.S. Government, and provides guidelines governing the correct implementation and deployment of these functions. FIPS 140-2 can be envisioned in a simple manner as defining two types of requirements: local requirements and algorithmic requirements.<sup>1</sup> Examples of local requirements include cryptographic boundaries and random bit generators. Local requirements have no implications for interoperability; they only have implications for the correctness of implementation or deployment. For example, the output of a FIPS approved random bit generator will appear to any computationally bounded party as a bit stream that is computationally indistinguishable from a true random bit stream.<sup>2</sup> Examples of algorithmic requirements include implementing symmetric key encryption using AES and hashing using SHA-1. These requirements have interoperability implications, because the communication protocols utilizing algorithms requires that their outputs in different implementations be identical. FIPS 140-2 does not address algorithmic interoperability directly. Instead, it defines known-answer tests for the cryptographic algorithms it approves. This means that each algorithm must operate on known inputs to produce known outputs. There is an indirect interoperability implication of these known-answer tests. In particular, every correct implementation must output the same bit pattern for each input in each known-answer test.

On January 21, 2005, NIST issued an updated implementation guidance document for FIPS 140-2. Section 7.2 of this update addresses IEEE 802.11i. It indicates that an IEEE 802.11i deployment can be certified and deployed for sensitive but unclassified use if it conforms to the following:

The IEEE Std 802.11i key derivation function is used to establish session keys from a shared secret constructed using an approved key establishment method. Annex D of FIPS 140-2 defines approved key establishment technique, including

---

<sup>1</sup> Jesse Walker, Intel Corp. "WPA2-and-FIPS" 2005.

<sup>2</sup> Jesse Walker, Intel Corp. "WPA2-and-FIPS" 2005.

Diffie-Hellman key establishment. EAP-TLS, which relies on Diffie-Hellman key agreement, is such a technique;

AES-CCM as defined in IEEE Std 802.11i is used to protect the data exchanged.

## **WPA and WPA2: Interoperability Certifications from Wi-Fi Alliance**

The Wi-Fi Alliance is a trade association that promotes the adoption of IEEE Std 802.11 technology through marketing and through interoperability testing. Products implementing IEEE Std 802.11i that are certified as interoperable are called WPA2 compliant. The Wi-Fi Alliance has conducted WPA2 certification since September 2004, and WPA2 will be required for any Wi-Fi Alliance certifications in April 2006.

WPA addresses the weaknesses of original WEP security resulting from WEP's imperfect encryption key implementation and its lack of authentication. Using TKIP, it brings an enhanced encryption algorithm, and with IEEE 802.1X/EAP authentication it brings standards-based mutual authentication, to Wi-Fi networks. Together, TKIP encryption and mutual authentication insulate the Wi-Fi network from a variety of threats when WPA-Enterprise mode is used.

Both WPA and WPA2 protect the wireless network from a variety of threats, including lost or stolen devices and hacker attacks such as 'man-in-the-middle', authentication forging, replay, key collision, weak keys, packet forging, and 'brute-force/dictionary' attacks.

WPA2 offers advanced protection from wireless network attacks. Using AES, government grade encryption and IEEE 802.1X/EAP authentication WPA2 provides stronger standards-based mutual authentication and advanced encryption to protect the Wi-Fi network from a variety of threats and attacks. WPA2 is the second generation of WPA security; providing enterprise and consumer Wi-Fi® users with a high level of assurance that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard and is eligible for FIPS 140-2 compliance. WPA2 is effectively the commercial certification of an implementation of 802.11i. WPA and WPA2 ensure interoperability within a large body of commercially-certified COTS wireless equipment. So it can be seen that WPA2 is desirable in any fielded wireless equipment if cost is an issue and interoperability with multiple vendors, in order to take advantage of a competitive marketplace, is a goal.

The WPA2 Enterprise interoperability test suite requires that products demonstrate interoperability of the following when used together:

EAP-TLS was compulsory for WPA2 Enterprise products certified prior to April 15, 2005; for products certified after this date, EAP-TLS testing is compulsory if the product can support EAP-TLS. The only products that might not support EAP-TLS are tightly integrated systems that do not support software upgrades by

a third party, such as some cell phones intended for, e.g., the 3G market. Non-tightly integrated products like most laptop and PDU adapters still must support EAP-TLS to receive WPA2 certification. 3eTI wireless products implement industry standard and WPA2 certified EAP-TLS

IEEE Std 802.11i key derivation from the symmetric key established by EAP-TLS;

AES-CCM, using the 128 bit key derived by 802.11i key derivation.

The test configuration for any product that supports EAP-TLS conforms exactly to the approved configuration specified by Clause 7.2 of the FIPS 140-2 implementation guidance document of January 21, 2005.

## **The Best Value: FIPS 140-2, 802.11i and WPA2 in the 3eTI Product Line**

This paper has described the primary functions of 802.11i and mentioned how 3eTI wireless access points, client devices, and security server products implement these main functions (EAP-TLS, 802.1X, 4-way handshake, AES CCMP) using standards-based, interoperable code. WPA2 certification further ensures this quality and effectively guarantees an interoperable, non-proprietary 3eTI wireless security product line (AP, clients, SS). 3eTI was the first company to take its 802.11i building block (AES CCM) through official NIST certification. Today, 3eTI 802.11i products are in the FIPS 140-2 prevalidation pipeline. So together, the combination of FIPS 140-2 security mechanisms, coupled with 802.11i and WPA2 interoperability, ensure a highly secure, non-proprietary wireless 802.11 solution for enterprise customers and the U.S. Navy sponsor.